BÁO CÁO BÀI TẬP

**Môn học: Bảo mật Web và Ứng dụng**

**Kỳ báo cáo: Thi cuối kỳ CTF**

**Tên chủ đề: Thi cuối kỳ CTF**

*GV: Nghi Hoàng Khoa*

*Ngày báo cáo: 2/6 /2023*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT213.N21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Võ Anh Kiệt | 20520605 | 20520605@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** | **Người đóng góp** |
| 1 | Kịch bản 01 | 100% |  |
| 2 | Kịch bản 02 | 100% |  |
| 3 | Kịch bản 03 | 100% |  |
| 4 | Kịch bản 04 |  |  |
| 5 | Kịch bản 05 |  |  |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

## Kịch bản 01

Vào discord lấy flag

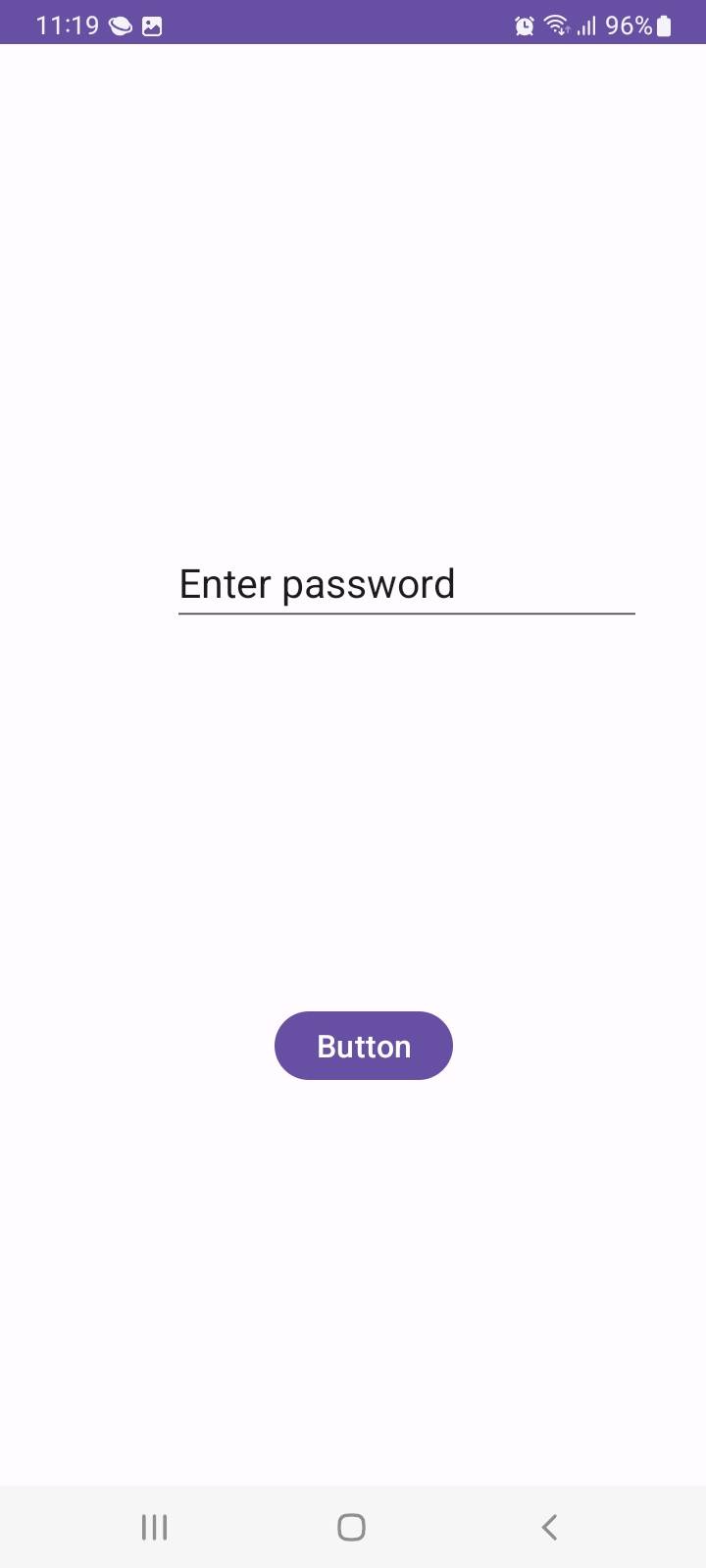
A screenshot of a computer

Description automatically generated

flag{tk4\_d3\_qj0t\_m0\_h0j\_r0j\_tr3n\_tr4nq\_s4ck\_c0n\_h0n\_qj0t\_nu0c\_m4t\_r0j\_tr3n\_d3\_tkj}

## Kịch bản 02

Đầu tiên ta tải file về và cài đặt



Ta thấy đây cần 1 password, vậy ta thực hiện decode ra, ở mục /res/values ta có được thông tin no\_one\_can\_escape\_from\_me

A picture containing text, screenshot, software, multimedia software

Description automatically generated

Tiếp tục thực decode bằng 1 tool khác ta có đoạn code sau

A screenshot of a computer screen

Description automatically generated with medium confidence

Với 2 đoạn code này ta thấy được chương trình đang thực hiện các thao tác như cộng, xor để thực hiện tạo mật mã, vậy ta sẽ thực hiện code lại với thao tác trừ và xor để thực hiện tìm password (giải thích code trong comment)

//import libraries

import java.util.Random;

//class main

class crack

{

    //public static void main

    public static void main(String[] args) {

        //create new random generator

        Random generator;

        //create new instance

        generator = new Random(105L);

        //declare variables from code give in decoder

        String firstString = "something\_that\_nobody\_can\_touch";

        String secondString = "no\_one\_can\_escape\_from\_me";

        int[] givenArray = {130, 96, 129, 40, 7, 253, 245, 36, 212, 199, 227, 87, 135, 195, 41, 87, 159, 156, 89, 154, 56, 188, 132, 161, 238, 9, 236, 9, 98, 231, 223, 209, 104, 207, 41, 149, 64, 154, 144, 60, 169};

        //loop through the array and print the flag

        for (int i = 0; i < givenArray.length; i++) {

            //get the last char from the array by using xor operation the given array with generated values

            int lastChar = (givenArray[i] ^ ((char)generator.nextInt() & 255));

            //get the ascii number from the last char by using xor operation the last char with the second string then subtract the first string

            int asciiNumber = ((lastChar ^ secondString.charAt(i % secondString.length())) - firstString.charAt(i % 31));

            //change the ascii number to the character and store it in a variable

            char piceOfFlag = (char)asciiNumber;

            //print the flag

            System.out.print(piceOfFlag);

        }

    }

}

Sau đó ta thực hiện chạy chương trình thì ta có được flag

A screen shot of a computer

Description automatically generated with medium confidence

Flag: flag{4ndr0id\_r3v\_5ucks55555555\_@$#&#$^#$}

## Kịch bản 03

Đầu tiên ta vào trang web thì không thấy gì bất thường

A screenshot of a web page

Description automatically generated with low confidence

Tiếp tục ta sẽ sử dụng burp suite để bắt gói tin và gửi vào repeater

A screenshot of a computer

Description automatically generated

Ta sẽ sửa /register.php thành index.php để xem có gì không thì ta vào được các note và thực hiện xoá session ID

A screenshot of a computer

Description automatically generated with medium confidence

Tiếp tục chỉnh sửa thành /index.php?note=1.txt thì ta xem được nội dung note

A screenshot of a computer

Description automatically generated with medium confidence

Tiêp tục sửa thành ../../../../../../etc/passwd thì ta có thể xem được nội dụng bên dưới, thì thấy được ta có thể vào được các file của hệ thống

A screenshot of a computer

Description automatically generated with medium confidence

Sau đó ta cần tạo 1 tài khoản với username: <?php system('../../../../../readflag')?> và password bất kỳ. Do trong gợi ý đã có 1 chương trình C tên là readflag nên ta sẽ để read flag và truyền vào hệ thống 1 câu lệnh để đọc flag

A screenshot of a web page

Description automatically generated with low confidence

Thực hiện login và lấy cookie của lấy flag

A screenshot of a computer

Description automatically generated with medium confidence

Cuối cùn sử dụng burp suite và phần GET thành /index.php?note=../../../../../../tmp/sess\_47fb9b1a7a75d326618a5660315734fa và ta có được flag

A screenshot of a computer

Description automatically generated with medium confidence

Giải thích: Do hệ thống không lọc gói tin đầu vào và việc xoá sessions ID thì ta vẫn vào được. Từ đó ta sẽ tạo 1 tài khoản có câu lệnh gọi flag và thực hiện đăng nhập vào và lấy session ID. Sau đó sử dụng vào sessions ID để gửi burp suite để lấy flag

Flag: flag{racing\_racing\_and\_you\_pwned\_me}

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

*Ví dụ: [*NT101.K11.ANTT*]-Session1\_Group3.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)